MaineCare Services
An Office of the
Department of Health and Human Services

Paul R. LePage, Governor   Mary C. Mayhew, Commissioner

Department of Health and Human Services
MaineCare Services
11 State House Station
Augusta, Maine 04333-0011
Tel. (207) 287-2674
Fax (207) 287-2675; TTY (800) 423-4331

Protect Patient Health Information:

Security Risk Analysis Tip Sheet

The following information has been compiled from the Centers for Medicare & Medicaid Services (CMS) and the Office for Civil Rights (OCR) to provide guidance to eligible professionals (EPs) and eligible hospitals (EHs) regarding the meaningful use (MU) measure **Protect Patient Health Information**.

In order to be deemed a meaningful user of certified EHR technology (CEHRT) and receive an EHR incentive payment, providers must attest to having met the Protect Patient Health Information measure. To meet this measure, EPs and EHs must conduct or review a **security risk analysis** (SRA) in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained in CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.

There are numerous methods of performing risk analysis and there is no single method or “best practice” that guarantees compliance. Although there is no specified method that guarantees compliance, there are several elements a risk analysis must incorporate, regardless of the method employed.

Requirement	Explanation	Regulation Reference 45 C.F.R §§	Source
Time Period	**Program Year 2014 and beyond:** The SRA has to be completed by **the provider’s attestation date**. The SRA can be completed prior to the MU reporting period, but no earlier than October 1 or January 1 (EH and EP respectively) of the EHR reporting year. If the provider’s attestation date is after the EHR reporting year (attested during tail period), the SRA submitted cannot be used in the attestation for the next program year. *For example, an EP attested on January 30,*	164.306(e), 164.316(b)(2)(iii)	CMS FAQ10754

Requirement	Explanation	Regulation Reference 45 C.F.R §§	Source
	2016 for a Program Year 2015 incentive payment and use the SRA completed January 15, 2016. The EP ***cannot*** *use this same SRA to meet the SRA requirement to also receive a Program Year 2016 incentive payment. The EP must conduct a new SRA or update the previous SRA in order to receive the Program Year 2016 incentive payment.*		
Physical Safeguards	According to the CMS tip sheet, the SRA should not be limited to just the EHR system (technical aspect). *(Examples include but are not limited to: computer equipment, your facility and other places where patient data is accessed, and portable devices)*	164.308, 164.310, 164.312	CMS SRA Tip Sheet
Administrative Safeguards	According to the CMS tip sheet, the SRA should not be limited to just the EHR system (technical aspect). *(Examples include but are not limited to: designated security officer, workforce training and oversight, controlling information access, and periodic security reassessment)*	164.308, 164.310, 164.312	CMS SRA Tip Sheet
Technical Safeguards	Technical safeguards should include controls on access to the EHR system and other electronic sources of ePHI.	164.308, 164.310, 164.312	CMS SRA Tip Sheet
Asset Inventory	The SRA should identify where all e-PHI is stored, received, maintained or transmitted. The asset inventory is used to determine the scope of the security risk analysis.	164.306(a), 164.308(a)(1)(ii)(A), 164.316(b)(1)	Office of Civil Rights Guidance, page 5

Requirement	Explanation	Regulation Reference 45 C.F.R §§	Source
Threats/ Vulnerabilities	Organizations must identify and document reasonably anticipated threats to e-PHI. Organizations may identify different threats that are unique to the circumstances of their environment. Organizations must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI.	164.306(a)(2), 164.308(a)(1)(ii)(A), 164.316(b)(1)(ii)	Office of Civil Rights Guidance, page 3
Current security measures	Organizations should assess and document the security measures an entity uses to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly.	164.306(b)(1), 164.308(a)(1)(ii)(A), 164.316(b)(1)	Office of Civil Rights Guidance, page 5
Likelihood of threat occurrence	The Security Rule requires organizations to take into account the probability of potential risks to e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).) The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Rule requires protection against because they are "reasonably anticipated."	164.306(b)(2)(iv), 164.308(a)(1)(ii)(A), 164.316(b)(1)(ii)	Office of Civil Rights Guidance, page 6
Potential impact of threat occurrence	The Rule also requires consideration of the "criticality," or impact, of potential risks to confidentiality, integrity, and availability of e-PHI. An organization must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. An entity may use either a qualitative or quantitative method or a combination of the two methods to measure the impact on the organization.	164.306(a)(2), 164.308(a)(1)(ii)(A), 164.316(b)(1)(ii)	Office of Civil Rights Guidance, page 6

Requirement	Explanation	Regulation Reference 45 C.F.R §§	Source
Level of risk	Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.	164.306(a)(2), 164.308(a)(1)(ii)(A), 164.316(b)(1)	Office of Civil Rights Guidance, page 6
Final report	The Security Rule requires the risk analysis to be documented but does not require a specific format.	164.316(b)(1)	Office of Civil Rights Guidance, page 7
Action plan	The SRA should include a list of corrective actions to be performed to mitigate each risk level. Any security updates and deficiencies that are identified in the review should be included in the provider's risk management process and implemented or corrected as dictated by that process.	164.306(e), 164.316(b)(2)(iii)	Office of Civil Rights Guidance, page 6
	All deficiencies do not have to be mitigated prior to attestation. The EHR incentive program requires correcting any deficiencies (identified during the risk analysis) according to the timeline established in the provider's risk management process, not the date the provider chooses to submit meaningful use attestation. The timeline needs to meet the requirements under 45 CFR 164.308(a)(1), including the requirement to "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [45 CFR]§164.306(a)."	164.306(e), 164.316(b)(2)(iii)	CMS FAQ10754